UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/706,871	11/12/2003	Nicholas Stamos	3602.1000-002	6738

21005 7590 02/16/2010

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER	
MURDOUGH, JOSHUA A	

ART UNIT	PAPER NUMBER
3621	

MAIL DATE	DELIVERY MODE
02/16/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/706,871	STAMOS ET AL.	
	Examiner	Art Unit	
	JOSHUA MURDOUGH	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 October 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Acknowledgements

1. This action is responsive to Applicants' above noted RCE and associated amendments received 13 April 2009.

2. This action has been assigned paper number 20100125 for reference purposes only.

3. Claims 1-22 are pending.

4. Claims 1-22 have been examined.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-22 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claims 1 and 12 are rejected as being indefinite because the relationship between the parts cannot be understood by one of ordinary skill in the art. Claim 1 recites, "defining a point-of-use security perimeter" and "use of the digital asset outside of the security perimeter." If the security perimeter is based on the point-of-use, how can the digital asset be used outside of the perimeter? As presently presented, the client device appears to be both within and outside of the security perimeter. Similar limitations are present in claim 12. Claim 12 is rejected under the same basis.

8. The Examiner finds that because particular claims are rejected as being indefinite under 35 U.S.C. §112 2nd paragraph, it is impossible to properly construe claim scope at this time.

However, in accordance with MPEP §2173.06 and the USPTO's policy of trying to advance prosecution by providing art rejections even though these claim are indefinite, the claims are construed and the art is applied as much as practically possible.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-5, 7, 8, 10-13, 15, 16, 18, 19, 21, and 22, as understood by the Examiner, are rejected under 35 U.S.C. §102(e) as being anticipated by Carter et al. (US 2003/0051026) ("Carter").

11. As to claim 1, Carter shows:

An agent process for controlling access to digital assets in a network of data processing devices, the process comprising:

defining a point-of-use security perimeter **114** that includes the operating system kernels of two or more data processing devices (protected servers, each server has an operating system and each operating system has a kernel inherently, Figure 1);

defining one or more policy violation predicates (Paragraphs 0775-0783) that serve to implement policy logic and that are asserted at the point-of-use of a digital asset

upon an occurrence of a possible risk of use, outside of the security perimeter of a digital asset by an end user (Paragraphs 0787-0791 and tables included within);

sensing atomic events (listed after paragraph 0787) within an operating system kernel of a user client device ("workstation," Figure 1) (Paragraph 0810), the atomic events being low level kernel events and being sensed upon activities related to authorized access (Paragraph 0811) (through switch controlled by the Network Surveillance and Security System, "NSSS" **18**) to a digital asset (located on a protected server within group **114**) by the end user of the user client device;

aggregating multiple atomic level events to determine a combined event (Paragraph 0435); and

asserting a policy violation predicate upon an occurrence of a combined event that violates a predefined digital asset usage policy that indicates a risk of use of the digital asset outside (inherent because the workstation is outside of the secure switch) of the security perimeter (Paragraph 0435).

12. As to claim 12, Carter shows:

A system for controlling access to digital assets in a network of data processing devices, the system comprising:

a digital asset usage policy server **18** storing one or more digital asset usage policies (Paragraphs 0787-0791 and tables included within) programmed to be applied to a point-of-use security perimeter **114**, the security perimeter comprising the operating system kernels of two or more data processing devices (protected

servers, each server has an operating system and each operating system has a kernel inherently, Figure 1);

an atomic event sensor (things sensed are listed after paragraph 0787, therefore there is inherently a sensor), the sensor located within an operating system kernel (Paragraph 0810) within an end user client device ("workstation," Figure 1) and programmed to sense atomic events from within the operating system kernel (Paragraph 0810), the atomic events being low level kernel events and being sensed by the sensor upon actions relating to of authorized access (Paragraph 0811) (through switch controlled by the Network Surveillance and Security System, "NSSS" **18**) to one or more digital assets by an end user of the end user client device;

an atomic level event aggregator (Paragraph 0435) programmed to determine the occurrence of an aggregate event that comprises more than one atomic level asset access event (Id.); and

a policy violation detector programmed to determine whether an aggregate event has occurred that violates a predefined digital asset usage policy (Paragraph 0435) that indicates a risk of use of a digital asset outside the security perimeter (Paragraph 0224).

13. As to claims 2 and 13, Carter further shows:

the step of asserting the policy violation predicate is implemented in the operating system kernel of the client user device (Paragraphs 0810-0817) .

14. As to claim 3, Carter further shows:

preventing a user from accessing the digital asset if the policy predicate indicates a violated policy (Paragraph 1040).

15. As to claims 4 and 15, Carter further shows:

the preventing step includes an IRP intercept (Paragraph 0147, interrupt handler within the kernel).

16. As to claims 5 and 16, Carter further shows:

the combined event is a time sequence of multiple atomic level events (Paragraph 0224).

17. As to claims 7 and 18, Carter further shows:

asserting multiple policy violation predicates (Paragraph 0435) prior to indicating a risk of use of the digital asset outside of the security perimeter (Paragraph 0224).

18. As to claims 8 and 19, Carter further shows:

operates independently of application software (It is within the kernel, which is part of the Operating System, not the application software).

19. As to claims 10 and 21, Carter further shows:

the sensors, aggregators, and asserting steps operate in real time (Abstract, real time updating of the knowledge base requires that the sensors, aggregators, and asserting of predicates also operate in real time).

20. As to claims 11 and 22, Carter further shows:

determining the identity of a particular file in the asset access event (Paragraph 0162, In order to access the remote file through the local file, the system needs to determine the identity of the remote file.).

21. As to claim 14, Carter further shows

the policy violation detector is programmed to determine a violated policy type (Shown as classes of violations in the table following paragraph 0787).

Claim Rejections - 35 USC § 103

22. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

23. Claim 9, as understood by the Examiner, is rejected under 35 U.S.C. §103(a) as being unpatentable over Carter in view of Danieli (US 6,510,513).

24. As to claim 9, Carter shows all of the elements of claim 1, but does not directly show the notification of the user that they have violated a policy. Danieli teaches "alerting a user of the

client computer of the inappropriate use" (see claim 14). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Carter by adding the teachings of Danieli to make it known to the user that there was a violation, because the notification allows the user to know they have done something the system believes they should not, enabling them to justify their actions to a responsible party and possibly get the policy changed, if their actions were justified.

25. Claims 6, 17, and 20, as understood by the Examiner, are rejected under 35 U.S.C. §103(a) as being unpatentable over Carter in view of Admitted Prior Art.

26. As to claims 6, 17, and 20, Carter shows all of the elements except for the ability of the user to document their reason for the policy violation. It is considered admitted prior art that documenting the reason for an access is old and well known I the art. It therefore would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Carter to incorporate this functionality. The ability to document the reason at the time of the occurrence would provide for a record of what was done and why, saving the effort of finding the appropriate person to notify.

27. Claims 1-5, 7, 8, 10-13, 15, 16, 18, 19, 21, and 22, as understood by the Examiner, are *alternatively* rejected under 35 USC 103(a) by Carter in view of Danieli.

28. As to claims 1 and 12, the Examiner primary position that it is inherent in Carter that the digital asset is used outside of the perimeter because the workstation using the asset is outside of the secure switch (Figure 1). However if not inherent, it is the Examiner's alternate position that

Danieli clearly shows the process of securing a digital asset outside of the perimeter (Figure 6). Therefore, if not inherent, it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the teachings of Carter to include the external security method of Danieli in order to extend the range of control over the digital assets past the security perimeter.

29. As to claims 2 and 13, Carter further shows:

the step of asserting the policy violation predicate is implemented in an operating system kernel of the client user device (element 1018, figure 10) .

30. As to claim 3, Carter further shows:

preventing a user from accessing the digital asset if the policy predicate indicates a violated policy (Paragraph 1040).

31. As to claims 4 and 15, Carter further shows:

the preventing step includes an IRP intercept (Paragraph 0147, interrupt handler within the kernel).

32. As to claims 5 and 16, Carter further shows:

the combined event is a time sequence of multiple atomic level events (Paragraph 0224).

33. As to claims 7 and 18, Carter further shows:

asserting multiple policy violation predicates (Paragraph 0435) prior to indicating a risk of use of the digital asset outside of the security perimeter (Paragraph 0224).

34. As to claims 8 and 19, Carter further shows:

operates independently of application software (It is within the kernel, which is part of the Operating System, not the application software).

35. As to claims 10 and 21, Carter further shows:

the sensors, aggregators, and asserting steps operate in real time (Abstract, real time updating of the knowledge base requires that the sensors, aggregators, and asserting of predicates also operate in real time).

36. As to claims 11 and 22, Carter further shows:

determining the identity of a particular file in the asset access event (Paragraph 0162, In order to access the remote file through the local file, the system needs to determine the identity of the remote file.).

37. As to claim 14, Carter further shows

the policy violation detector determines a violated policy type (Shown as classes of violations in the table following paragraph 0787).

Response to Arguments

38. Applicant's arguments filed 7 October 2009 have been fully considered but they are not persuasive.

39. Applicants argue:

40. "Applicants respectfully submit that the language of Claims 1 and 12 in view of the specification would be understood by one of ordinary skill in the art and is not indefinite. As such, Applicants respectfully request withdrawal of the rejections of Claims 1-22 under 35 U.S.C. 112, second paragraph. Applicants would, of course, gladly consider any amendments that the Office may suggest regarding the point-of-use perimeter" (Remarks, Page 3, Paragraph 3).

41. Examiner's response:

42. Claims 1 and 12 are rejected for being indefinite because of the use of the descriptor "point-of-use' prior to "security perimeter." The descriptor "point-of-use" implies that the digital asset is to be used within the perimeter. Claim 1 indicates there is "a risk of use of the digital asset outside of the security perimeter." Because there is a risk of use outside the perimeter, one of ordinary skill in the art would understand that the actual point-of-use could be outside the security perimeter. Because the "point-of-use" can be outside of the security perimeter, the description of the security perimeter as a "point-of-use security perimeter" is inaccurate.

43. The Examiner's understanding of Applicants' intended invention is as follows:

a. A multi-device perimeter is established.

i. The digital assets are for use inside the perimeter.

ii. System/kernel events are monitored inside the perimeter.

iii. Events are looked at in context/combinations.

b. Security scripts/procedures regulate use of the digital asset.

iv. These scripts/procedures are enacted based on the context/combinations of the system/kernel events.

v. The intent of the scripts/procedures is to prevent use outside the perimeter.

44. If the description by the Examiner is what Applicants are trying to claim, the Examiner suggests the following as an example of language that will better set forth Applicants' invention and overcome the rejection under 112 2nd paragraph:

An agent process for controlling access to digital assets in a network of data processing devices, the process comprising:

defining a security perimeter;

the security perimeter includes two or more data processing devices in the network, each of the two or more processing devices containing an operating system kernel;

at least one of the two or more data processing devices being a user client device;

the security perimeter also containing a digital asset;

defining one or more policy violation predicates, the one or more policy violation predicates implementing policy logic controlling the use of the digital asset by the user client device;

sensing atomic events within the operating system kernel of the user client device;

the atomic events being low level kernel events and being sensed upon actions relating to authorized access to the digital asset by the end user of the user client device;

aggregating multiple atomic level events on the user client device to determine a combined event; and

asserting a policy violation predicate, at the user device, upon an occurrence of a combined event that violates the policy logic;

the policy logic violation corresponds a risk of use of the digital asset outside of the security perimeter.

45. The example claim above is derived from claim 1. The Examiner has attempted to better set forth the invention as understood while overcoming the rejection under 112 2nd paragraph. Additionally, the Examiner has searched this claim as suggested, and was unable to find prior art to reject it.

46. The Examiner again notes that the claims currently presented are subject to a rejection under 35 U.S.C. 112 2nd paragraph and are therefore subject to potentially unintended interpretations. Because of these interpretations, the arguments are not persuasive for the current claims.

Conclusion

47. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

48. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

49. Applicants are respectfully reminded that any suggestions or examples of claim language provided by the Examiner are just that—suggestions or examples—and do not constitute a formal requirement mandated by the Examiner. To be especially clear, any suggestion or example provided in this Office Action (or in any future office action) does *not* constitute a formal requirement mandated by the Examiner.

c. Should Applicants decide to amendment the claims, Applicants are also reminded that—like always—no new matter is allowed. The Examiner therefore leaves it up to Applicants to choose the precise claim language of the amendment in order to ensure that the amended language complies with 35 U.S.C. § 112 1st paragraph.

d. Independent of the requirements under 35 U.S.C. § 112 1st paragraph, Applicants are also respectfully reminded that when amending a particular claim, all claim terms must have clear support or antecedent basis in the specification. See 37 C.F.R. § 1.75(d)(1) and MPEP § 608.01(o). Should Applicants amend the claims such that the claim language no longer has clear support or antecedent basis in the specification, an

objection to the specification may result. Therefore, in these rare situations where the amended claim language does *not* have clear support or antecedent basis in the specification and to prevent a subsequent 'Objection to the Specification' in the next office action, Applicants are encouraged to either (1) re-evaluate the amendment and change the claim language so the claims *do* have clear support or antecedent basis or, (2) amend the specification to ensure that the claim language does have clear support or antecedent basis. See again MPEP § 608.01(o) (¶3). Should Applicants choose to amend the specification, Applicants are reminded that—like always—no new matter in the specification is allowed. See 35 U.S.C. § 132(a). If Applicants have any questions on this matter, Applicants are encouraged to contact the Examiner via the telephone number listed below.

50. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOSHUA MURDOUGH whose telephone number is (571)270-3270. The Examiner can normally be reached on Monday - Thursday, 7:00 a.m. - 5:00 p.m.

51. If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

52. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Joshua Murdough
Examiner, Art Unit 3621

/ANDREW J. FISCHER/
Supervisory Patent Examiner, Art Unit 3621